

Patent
62478-9100

REMARKS

Claims 1-76 have been cancelled. Claims 77-101 have been newly added. Applicant respectfully requests examination.

Applicant's invention provides a file management apparatus 10 that generates two independent encrypted file keys each of which can be used to decipher the same ciphertext. To generate the keys a user takes a portable key storage medium 20 and inserts it in the file management apparatus 10. The user also enters a password into the password input unit 101. The file management apparatus 10 takes the password and the key information on the key storage medium 10 and uses the password and key information to generate a first encrypted file key. The file management apparatus 10 also takes the key information and uses only the key information to generate a second encrypted file key. The file encryption unit 200 then uses the key information from the portable key storage medium 20 to encrypt a plain text file 401 into a ciphertext file for storage in a storage unit 400 along with the first and second encrypted file keys. To later unlock the ciphertext file 404, the user enters the password into the password input unit 301 providing the file management apparatus 10 with the information needed to decrypt the first encrypted file key 403 or the user inserts the key storage medium 20 in the management apparatus 10 providing file management apparatus 10 with the information needed to decrypt the second encrypted file key 404. Using the first encrypted file key 403 or the second encrypted file key 404 the decryption unit 305 decrypts the ciphertext file.

This dual encrypted file key system has many advantages. For example, if a user loses the key storage medium 20, the user can invalidate the key storage medium 20 for use in decryption of ciphertext files in the file management apparatus 10 by deleting the second encrypted file key. The user can then use the password to command the file management

Patent
62478-9100

apparatus 10 to decipher a ciphertext file. If the user forgets the password or the password is compromised, the user can invalidate the password by deleting the first encrypted file key. The user then can then use the portable key storage medium 20 to decipher ciphertext files.

The Office Action had applied the *Schneier* "Applied Cryptography" Second Edition textbook against the previous claim 17 and 57-75. Applicant has addressed both the 35 U.S.C. §112 issues and the *Schneier* reference in defining the present invention in the new claims 77-101.

Claim 77 captures the use of a first encrypted file key and a second encrypted file key reciting "a key encryption unit operable to generate a first encrypted file key by encrypting the original file key using a first password, generate a second encrypted file key by encrypting the original file key using the key information, and write the generated first and second encrypted file keys into the memory unit." This feature is not disclosed or suggested in *Schneier*.

The Office Action cites passages from pages 180 to 182 of *Schneier* (Office Action, Paragraph 4). These passages disclose that hard-to-remember keys can be stored in encrypted form using something similar to a key encryption key. For example, an RSA private key could be encrypted with a DES key and stored on disk. To recover the RSA key, the user has to type in the DES key to a decryption program (*Schneier*, Page 181 Paragraph 5).

The system described in *Schneier* lacks the recited key encryption unit that generates a first encrypted file key and a second encrypted file key. *Schneier* uses only one file key, the RSA key. The DES key is used to encrypt and recover the RSA key but the DES key cannot be used as a file key. This type of system does not provide the same functionality as Applicant's invention. For example, if *Schneier*'s DES key (password) is compromised the user may delete the RSA key and maintain system security. However, deletion of the RSA key makes it

Patent
62478-9100

impossible to recover an encrypted file. With Applicant's invention, if the password is compromised the user merely deletes the first encrypted file key and inserts the key storage medium to decrypt the second encrypted file key and uses the second file key to decrypt an encrypted file. Similarly if the storage medium is compromised, the user deletes the second encrypted file key and uses the password to decrypt the first encrypted file key and uses the first file key to decrypt the encrypted file.

Applicant provides a detailed disclosure about the first key encryption unit 102, the second key encryption unit 103, the first file key 403, the second file key 404 and the memory unit 400 (Application, Figure 2, page 10 lines 5-17, page 18 lines 1-6). The key storage medium 20, the file key generating unit 201, and the text encrypting unit 203 of Claim 77 can also found in Figure 2.

Claims 78 - 93 depend from Claim 77 and are patentable for the same reasons. Claims 78-79 and 81-87 also recite a registration unit 100 (Application, Figure 2, Page 28, Lines 9-18).

Claim 94 recites "a decrypting unit operable to generate a decrypted text by decrypting the ciphertext using either the first decrypted file key generated by the first key obtaining unit or the second decrypted file key generated by the second key obtaining unit". Claim 94 also recites "a deleting unit operable to delete either the first decrypted file key or the second decrypted file key." As explained above, *Schneier* device uses only a single file key, the RSA key. *Schneier's* DES key merely decipheres the encrypted RSA key. Thus, *Schneier* does not disclose a decryption unit or a deleting unit that decrypts or deletes a first and second encrypted file key.

The decryption unit 300 and the deleting unit are disclosed in detail (Application, Figure 2, Page 34 Line 17- Page 37 Line 12, Page 38 Lines 15-19, and Page 41 Lines 17-25). The key storage medium 20, the memory unit 400, the first key obtaining unit 302, the second key

Patent
62478-9100

obtaining unit 304 and a switch unit 303 are also disclosed, (Application, Figure 2, Page 35 Lines 1-15).

Claims 95 and 96 depend from claim 94 and are patentable for the same reasons. Claim 96 also recites a matching unit (Application, Page 44 Line 24, Page 45 Line 3).

Claim 97 recites the limitations of both Claim 77 and Claim 94 and is patentable for the same reasons as each of those claims.

Claims 98 and 99 recite a method and computer program for a file encryption apparatus. The method (program) is not disclosed or suggested in *Schneier*. The apparatus includes the portable key storage medium 20 and the memory unit 400. The method includes the steps of generating an original file key S222, generating ciphertext S223 and generating a first and second encrypted file key S226, S228 (Application, Figure 12).

Claim 100 and 101 recites a method and computer program for a file encryption apparatus. The apparatus includes the portable key storage medium 20 the memory unit 400. The method (program) includes the steps of generating a first decrypted file key S244, generating a second decrypted file key S246, switching between the keys S241, generating a decrypted text S247, and deleting the decrypted file key (Application, Figure 13, Page 38, Lines 15-19, and Page 41 Lines 17-25).

It is believed that the application is now in condition for allowance and early notification of the same is requested.

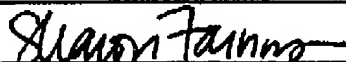
Patent
62478-9100

If the examiner believes that a telephone interview will help with the prosecution of the present case, the undersigned attorney can be contacted at the listed phone number.

I hereby certify that this correspondence is being
transmitted via facsimile to the USPTO at
571-273-8300 on April 28, 2006.


Very truly yours,
SNELL & WILMER L.L.P.

By: Sharon Farnus



Signature

Dated: April 28, 2006



Joseph W. Price
Registration No. 25,124
600 Anton Boulevard, Suite 1400
Costa Mesa, California 92626-7689
Telephone: (714) 427-7420
Facsimile: (714) 427-7799